PRIVACY IMPACT ASSESSMENT (PIA)

For the

Asset Management System (AMS)
US Army Medical Command - DHP Funded System

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☐ (2) Yes, from Federal personnel* and/or Federal contractors.

☒ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

☐	**New DoD Information System**	☐	**New Electronic Collection**
☒	**Existing DoD Information System**	☐	**Existing Electronic Collection**
☐	**Significantly Modified DoD Information System**		

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

☐	**Yes, DITPR**	Enter DITPR System Identification Number	
☐	**Yes, SIPRNET**	Enter SIPRNET Identification Number	
☒	**No**		

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

☐	**Yes**	☒	**No**

If "Yes," enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. Does this DoD information system or electronic collection require a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifier. PIA and Privacy Act SORN information should be consistent.

☒	**Yes**	☐	**No**

If "Yes," enter Privacy Act SORN Identifier A0001DAPE

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information.

This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

☐ **Yes**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. (If multiple authorities are cited, provide all that apply.)

(a) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records.

(c) DoD Components can use their general statutory grants of authority ("internal housekeeping") as the primary authority. The requirement, directive, or instruction implementing the statute within the DoD Component should be identified.

10 U.S.C. 1330 and E.O. 9397 (SSN).

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

The Asset Management System (AMS) is an automated bank support system that is capable of tracking personnel data on all individuals (government and contractors) assigned to the United States Army Medical Information Technology Center (USAMITC). The data captured is used by Human Resources, Resource Management, Security, Information Assurance, Training, Division/Branch Chiefs, and Procurement. The capability to track this information is a critical factor to the success of USAMITC operating as an organization and as an enterprise servicing others worldwide. The organization has the need to track management data that directly impacts on military, organizational, and personnel readiness reporting.

The following PII is collected: Name, Citizenship, Personal Cellphone number, Home Address, Emergency Contact, Other Names Used, Birth Data, Home Telephone Number, Social Security Number, Employee ID Number, Place of Birth, Security Clearance, Spouse Information, and Financial Information.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Three discreet potential privacy risks were considered in designing and developing AMS:

- Unauthorized Access
- Privacy and due Process Right Protection
- Unauthorized Disclosure

In response to the risk of unauthorized access to the sensitive information that records within AMS will contain, USAMITC takes a "defense in depth" approach to protecting this information. Physical safeguards (e.g., data stored on accredited servers in the USAMITC), technical safeguards (e.g., common access card and password protection) and procedural safeguards (e.g., physical access to data based on duty position) are employed in series to ensure only those personnel that demonstrate "need to know" can access information contained within AMS. In response to the risk of violating the rights of the individuals involved in the employee tracking process, USAMITC is relying on redundant and parallel protective steps to ensure the individual rights of all parties are vigorously protected. Data is only viewed by AMS users that require access to the information in the performance of their duties. In response to the risk presented by unauthorized disclosure of information contained, USAMITC requires that users of AMS receive information assurance awareness training in order to mitigate risks involved. This multi-faceted approach to safeguarding PII provides redundant protections to both the individual identities and institutions involved in the collection and management of this highly personal and sensitive information.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☒ **Within the DoD Component.**

Specify. PII is shared with personnel with a need-to-know within USAMITC.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

The employee can object to the collection of PII during the intake interview. In accordance with the Privacy Act Statement associated with this system, furnishing PII is voluntary, but failure to provide this information would prohibit commander/supervisor from contacting an individual during an emergency.

(2) If "No," state the reason why individuals cannot object.

j. Do individuals have the opportunity to consent to the specific uses of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe the method by which individuals can give or withhold their consent.

The employee has an opportunity to consent to the specific uses of their PII during the intake interview. The specific uses of their PII are addressed in the Privacy Act Statement associated with this system.

(2) If "No," state the reason why individuals cannot give or withhold their consent.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☐ **Other** ☐ **None**

Describe each applicable format.	AUTHORITY: 10 USC 3013 and E.O. 9397 (SSN) PRINCIPAL PURPOSES: To provide commanders and supervisors with emergency notification data other users with locator data. ROUTINE USES: Information will be used only within the assigned activity and will not be released to any other staff activity. MANDATORY OR VOLUNTARY DISCLOSURE AND EFFECT ON INDIVIDUAL OF NOT PROVIDING INFORMATION: Information is voluntary; however, failure to provide information would prohibit commander/supervisor from contacting an individual during an emergency.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.